Inspire Your Community

Text your neighbors. Call your child's school. Email your relative across the country. Encourage them to participate in **ShakeOut** and **America's PrepareAthon**!

Everyone needs a friendly reminder now and then, or maybe just a little help securing that bookcase to the wall. Be the positive inspiration your community needs!

https://community.fema.gov/

Family Preparedness

Have you heard? National Parents' Day is July 24. In observance of this occasion, we encourage you to take specific actions to prepare your family for emergencies. America's PrepareAthon! and the Ready Campaign highlight several ways you can prepare for the unexpected.

Some of these actions include:

- **Creating a family emergency communication plan**. Your family may not be together when disaster strikes, so it's important to plan ahead about how you will connect with each other;

- **Building a disaster supply kit**. A disaster supply kit is simply a collection of basic items your household may need in the event of an emergency. You may need to survive on your own after a disaster. This means having your own food, water, and other supplies in sufficient quantity to last for at least 72 hours. Local officials and relief workers will be on the scene after a disaster, but they cannot reach everyone immediately. You could get help in hours or it might take days; and

- **Practicing your emergency response plan.** Making emergency plans is great, but practicing your plan by conducting drills will help your family's response time when seconds count.

Disasters can be stressful for kids. Try to make emergency planning fun for children in your family! Visit ready.gov/kids for exciting games, quizzes, and other resources to help young children and teens understand the importance of being prepared.

Disasters also impact older adults. Visit ready.gov/seniors to learn more about preparing older Americans for the unexpected.

Natural Disasters and Severe Weather

Hurricane Readiness – (CDC)
http://www.cdc.gov/features/hurricanepreparedness/index.html

CDC Feature: Flood Safety Tips – (CDC)
http://www.cdc.gov/features/flood-safety/index.html

Food and Water Needs: Preparing for a Disaster or Emergency – (CDC)
emergency.cdc.gov/disasters/foodwater/prepare.asp

Health and Safety Concerns for All Disasters – (CDC)
emergency.cdc.gov/disasters/alldisasters.asp

Food Safety Before and After Disasters

Power outages can jeopardize the safety of the food stored in your home refrigerator or freezer. If you lose electricity, do you know how to determine if your food is safe to eat? The U.S. Department of Agriculture (USDA) offers tips to follow before and after a power outage to minimize loss of food and lower the risk of foodborne illness:

- Gather an emergency food supply of shelf-stable food, boxed or canned milk, bottled water, and canned goods;

- Have coolers and frozen gel packs on hand to keep refrigerated food cold if the power goes out longer than four hours;

- Buy an appliance thermometer for the refrigerator and freezer and a food thermometer to help you know if the food has stayed at a safe temperature during an outage;

- Throw out any perishable food items such as meat, poultry, fish, eggs, and leftovers that have been exposed to temperatures above 40 degrees Fahrenheit for more than two hours;

- Use a food thermometer to test the temperature of food – never taste it! You can't rely on appearance and odor to determine whether food is safe; and

- Discard any items in the refrigerator that have come into contact with raw meat juices.

Keep in mind that your refrigerator will keep food cold safely for about four hours if it is unopened. A full freezer will hold the temperature for approximately 48 hours (24 hours if it is half full) if the door remains closed.

Did you know that a flood or fire can also impact the safety of food in your home? Be sure to check out the FAQs on the USDA website about keeping food safe after these emergencies.

Preparedness for People with Disabilities and Others with Access and Functional Needs

This year marks the 26th Anniversary of the Americans with Disabilities Act (ADA). Signed into law in 1990 by President George HW Bush, the ADA prohibits discrimination and mandates equal opportunities for people with disabilities in employment, state, and local government services, public accommodations, commercial facilities, transportation, and telecommunication.

If you or someone you know has a disability or access or functional needs, be sure to take additional steps to stay safe, healthy, mobile, and independent during a disaster.

Find out about assistance programs that may be available in your community and register in advance with your local office of emergency services, non-profit groups, and health departments.

Stay mobile and independent by including items in your disaster supply kit that meet your needs such as:

- Extra eyeglasses and hearing aids;
- Medical prescriptions;
- Batteries and chargers for assistance devices; and
- Written descriptions of service needs.

Looking for more ways to plan for people with disabilities and others with access and functional needs? Check out this video from the *Ready* Campaign and the Ad Council. The video is for all communities and shows people with disabilities taking charge to prepare themselves and their families for emergencies. The video provides equal access and includes open captioning, a certified deaf interpreter, and audio description for viewers who are blind or have low vision.

SBA
U.S. Small Business Administration

Webinar | Protecting Your Business Data in Todays Inter-Connected World

Register | Thursday, July 28, 2016 | 8:30am - 9:30am PST

The threat landscape in cyber-space keeps evolving. Cloud technologies are designed to continuously identify and mitigate risks, and can help small businesses leverage the best of breed security and privacy capabilities, while focusing on their core competencies.

Join this webinar to learn more about how cybersecurity threats are evolving, what risks they pose, and best practices to protect your business information in the digital age.

Beware of Olympics Cyber Scams

As the 2016 Summer Olympic Games quickly approach, athletes across the globe are preparing to compete and hopefully bring a medal back to their home country.

However, athletes aren't the only ones gearing up for the Olympics – cybercriminals are busy looking to exploit excitement around the Olympics to take advantage of unsuspecting consumers and steal their money and personal information.

These 'cyber pickpockets' will use a variety of tactics to try and trick people into handing their money over online, making it critical to stay extremely vigilant. Hackers and identity thieves have been known to exploit high profile events like the Olympics through use of phishing emails and websites to target people looking to purchase tickets, merchandise, or stream video online. The Better Business Bureau found that during the 2014 Winter Olympics in Sochi, a search on eBay for "Sochi 2014" found 5,693 results, some of which were fraudulent even including a fake "Olympic Torch Sochi 2014" for $7,000.

The Stop.Think.Connect.™ Campaign encourages you to be on the lookout for the following common scams during the Olympics season and throughout the year:

Phishing Emails

Scammers use emails to collect personal and financial information or infect your machine with malware and viruses. Cybercriminals use legitimate-looking emails that encourage people to click on a link or open an attachment. The email they send can look like it is from an authentic, Olympics-related organization or legitimate retailer.

How to protect yourself: When in doubt, throw it out. Links in email and online posts are often the way cybercriminals compromise your computer. If it looks suspicious – even if you know the source – it's best to delete or, if appropriate, mark it as "junk email." Contact the company directly (via phone) to check the email's legitimacy.

Counterfeit Merchandise

Regardless of if you are physically at the Olympic Games in Rio de Janeiro or not, scammers will try to take advantage and sell you fake merchandise and tickets online.

How to protect yourself: Shop only at reputable online retailers, ideally only the official Olympics website. Look for the padlock symbol or for URLs that start with "https" or "shttp." For auction websites, be sure to check the sellers' reviews. Also, be sure to always pay for online purchases with a credit card, which offers greater protection than a debit card.

"You've Won" Scams

If you unexpectedly receive an email telling you that you have won a prize, lottery, or sweepstakes (for example, free tickets to the Olympics games), it may be an online scam. Though the person seems excited for you to collect your winnings, if they then tell you there is a fee or tax to claim the prize and request your credit card or bank account information, it's likely a trick.

How to protect yourself: Think before you act. Be wary of communications that implore you to act immediately, offer something that sounds too good to be true, or ask for personal information.

To report suspected phishing attempts, consumers have three resources to use. Consumers can visit the Anti-Phishing Working Group (APWG) at www.apwg.org. In addition, the United States Computer Emergency Readiness Team (US-CERT) also collects phishing email messages and website locations to help people avoid becoming victims of phishing scams. To report suspected phishing attempts to DHS, visit www.us-cert.gov/report-phishing. Finally, consumers can visit the National Cyber Security Alliance's Spam and Phishing page for more information on how to protect yourself against these attacks.

For more information and tips for staying safe year-round, please visit DHS.gov/StopThinkConnect.

HERE'S HOW TO STAY SAFE ONLINE THIS SUMMER

When you think about summer safety, the things that come to mind are likely sunscreen, umbrellas, and lifeguards. However, as we all lead increasingly connected and digital lives, it is just as important to take steps to protect yourself online throughout the summer as it is to remember to reapply your SPF.

Summer is a time for adventure. Many Americans will be traveling and kids across the country are out of school with extra free time. The more we access the Internet on-the-go, the more

increased cyber risks we face. Protecting yourself from these risks by following simple steps is critical. Just as a lifeguard is responsible for protecting everyone in a pool, you are responsible for ensuring your safety online while on-the-go or at home.

The Stop.Think.Connect. Campaign encourages all Americans to follow these five simple steps to protect yourself whenever accessing the Internet from your mobile device:

- **Enable multi-factor authentication.** A multi-factor authentication requires that you use your password in conjunction with an additional piece of information (commonly a one-use password that is voided as soon as you use it, such as a PIN sent to your mobile device). Even if cybercriminals have your password, they won't be able to access the account without the second component if multi-factor authentication has been used.
- **Keep software up to date.** Install updates for apps and your device's operating system as soon as they are available. Keeping the software on your mobile device up to date will prevent attackers from being able to take advantage of known vulnerabilities.
- **Guard your mobile device.** In order to prevent theft and unauthorized access, never leave your mobile device unattended in a public place and lock up your device when it is not in use.
- **Be careful what you post and when.** Wait to post pictures from trips and events so that people do not know where to find you. Posting constantly and in real time of where you are also reminds others that your house is empty, leaving you more vulnerable to burglary.
- **Disable remote connectivity.** Some mobile devices are equipped with wireless technologies, such as Bluetooth, that can connect to other devices. Disable these features when they are not in use.

For more information and tips for staying safe online this summer and throughout the year, please visit DHS.gov/StopThinkConnect.

FTC RELEASES NEW IMPOSTER SCAM VIDEOS

The Federal Trade Commission (FTC), a Stop.Think.Connect. Campaign partner and the nation's consumer protection agency, has released four new videos to help consumers avoid imposter scams.

Imposter scams happen when a person pretends to be someone you trust and tries to convince you to send them money. In fact, imposter scams were the 3rd most common complaint the FTC received last year**.**

To help people avoid imposter scams, the FTC has four new videos – on IRS imposters, tech support schemers, online dating con artists, and the "grandkid" scam. The series of one-minute videos show how people are targeted, how to spot the scam, and where to report it. Check them out at ftc.gov/imposters or ftc.gov/impostores in Spanish.

Along with the videos, the FTC also has four new articles on imposter scams. The articles are part of FTC's Pass It On campaign, which encourages older adults to talk with family, friends, and neighbors about avoiding common scams. Free copies are available to order at ftc.gov/bulkorder.

Cyber Info – Links

- **5 'Mr. Robot' Hacks That Could Happen in Real Life**

- **Macs and iPhones have a Stagefright-style bug!**

- **Ransomware gang: How can I extort you today?**

Minding Your Own Business

What are you doing at your workplace to get prepared for earthquakes? Would your business be able to survive and recover from a disaster? Business continuity is an issue all workplaces face, big or small, private, public, or non-profit. The good news is that there are resources to help guide how your business prepares to survive and recover. Start today by walking around and **identifying potential hazards**, or train your employees on **how to use a fire extinguisher**.

The difference between an organization that survives a disaster and those that fail, is taking action before disaster strikes! About 40% of businesses without a disaster plan will fail after an event, with another 25% closing a year later. At **ResilientWorkplace.org**, you can find more information about the **QuakeSmart Community Resilience Program**, the **Disaster Resilient Business toolkit**, and the **Seven Steps to a Disaster Resilient Workplace.**

Please cut and past the following link into your browser:

http://www.earthquakecountry.org/downloads/7_Steps_to_a_Disaster_Resilient_Workplace.pdf

Preparing for the Flu in your Community

CDC partnered with the National Influenza Vaccination Disparities Partnership(NIVDP) to create a toolkit for community organizations to reach underserved populations. The toolkit is packed with information to become better informed about influenza and the influenza vaccine. The kit is also intended to help increase awareness about the importance of flu vaccination, specifically for high risk groups such as children, pregnant women, the elderly, and individuals with chronic health conditions.

Download the toolkit and find out how you can help flu vaccination efforts in your community:

https://lnks.gd/l/eyJhbGciOiJIUzI1NiJ9.eyJlbWFpbCI6InJ1c3NlbGwuZm94QGZlbWEuZGhzLmdvdiIsImJ1bGxldGluX2xpbmtfaWQiOiIxMDUiLCJzdWJjcmliZXJfaWQiOiNTkzNDg3MzM2IiwibGlua19pZCI6Ijg3MTMyODI1IiwidXJpIjoiYnAyOmRpZ2VzdCIsInVybCI6Imh0dHA6Ly93d3cuY2RjLmdvdi9mbHUvcGRmL25pdmdvbml2ZHAtcmVzb3VyY2Uta2l0LTIwMTUucGRmIiwiYnVsbGV0aW5faWQiOiIyMDE2MDcxMi42MTQyOTEzMSJ9.kmcC5EUDcfdkImbaBRRJ7kTLWTPUNue1YyeCe9pC3to

Zika Topic of the Week: Stay Healthy on the Road to Rio!
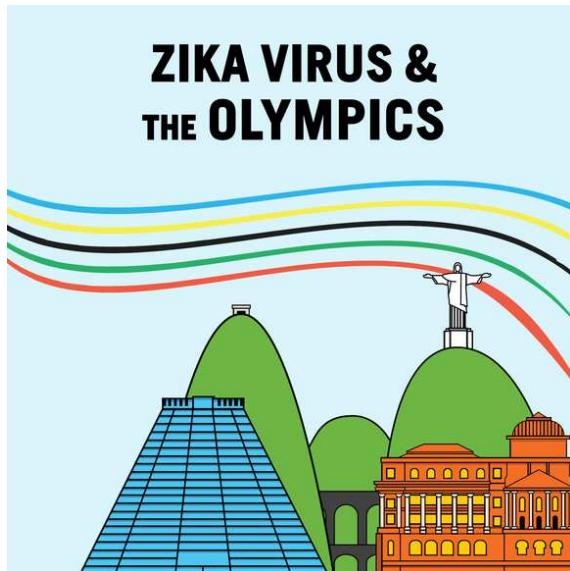
Are you headed to the 2016 Rio Olympic or Paralympic games? Whether you're a Team USA competitor or fan, you can maintain a strong defense against health risks with good travel preparation and practices. While in Brazil, you could face a variety of health risks, and Zika is one of them. CDC's travel health tips can help you, your family, and your community back in the U.S. to stay protected. Zika is one tough opponent everyone wants to beat. We want you to stay healthy during the games and beyond. With the right steps you can bring home medals and memories, not illness!

Weekly CERC/ZIKA Teleconference

To address the communication concerns and needs of state, local, and territorial health communicators, as well as partner organizations, CDC is hosting a series of Crisis and Emergency Risk Communication (CERC) teleconferences related to Zika issues.

These teleconferences are held on a weekly basis from **1-2 pm (Eastern Time).** Each week, a new CERC topic will be presented as it relates to Zika.

July 26 – CERC, Zika, Stigma, and Working with the Media - During this week's Zika Crisis and Emergency Risk Communication discussion we will explore how to work with the media during a crisis. Learn what to expect when the world is directing its media attention on your community. We will share media dos and don'ts for your official response.

Audio Conference Access Information:

1-800-369-1662 (U.S. Callers)

1-203-827-7082 (International Callers)

Passcode: 3266392

All calls will be recorded and posted to our website.

Presentation slides for this teleconference will be available on our website: https://emergency.cdc.gov/cerc/zika-teleconferences.asp

Emergency Management and Health Communication Tips

Responding to Rumors and Misinformation

Most emergencies are susceptible to communication errors. Misunderstandings, mistrust, and simple mistakes may cause conflicting messaging to emerge. For crisis communicators, it's important to understand when and how wrong messages should be corrected.

While many messaging errors might have little to no impact on people affected by a disaster, some rumors and misinformation can be very destructive.

- Misunderstandings can cause confusion. People may not know what to do if they don't feel they have enough information or are unable to interpret the information that is available to them.
- Mistrust may make rumors seem reasonable. If people affected by a crisis don't trust your organization, they may not trust your advice. The public could believe incorrect information if they feel its source is more credible than you.
- Simple mistakes may account for other emergency errors. Oversights—including typos and lack of fact checking—may lead people to misread messaging.

Misleading communication might promote harmful behaviors that increase personal and public health risks. Inconsistent guidance can also undermine the credibility of your organization.

As a crisis communicator, you must know when and how to address these communication errors. While it may not be realistic to respond to every rumor, misinformation that can be damaging should be corrected. The following steps can help you address myths, rumors, and misconceptions:

- Monitor traditional and social media and conduct environmental scanning to identify possible misinformation.
- Dispel rumors by immediately providing accurate information through appropriate channels, including

  * Media

  * Social media

  * Partner organizations

  * Print and website content disseminated by your organization

- Regularly update information outlets with current information to help them avoid speculation.

Effective communication—including managing misinformation—can help reduce and prevent public health risks in emergency situations. For the more details on communicating during crises, please see Crisis and Emergency Risk Communication, 2014 Edition, at http://emergency.cdc.gov/cerc/resources/pdf/cerc_2014edition.pdf.

CDC Emergency Preparedness Online Training

CERC Online Training

CERC Online Training Module(https://emergency.cdc.gov/cerc/cerconline/training/index.html)

Objectives:

At the conclusion of the training, the participant will be able to do the following:

*Explain Crisis and Emergency Risk Communication (CERC) principles.

*Describe the psychology of a crisis and the type of messages each audience needs.

*Define core concepts of crisis communication planning.

*List techniques to communicate

CERC Pandemic Influenza Training

Objectives

After completing the training, the participant will be able to do the following:

- Describe the psychology of a severe pandemic.
- Describe how to meet the public's needs through effective messages.
- Explain why stigmatization occurs.
- Explain strategies officials can use to respond to stigmatization.
- Recognize the importance of strengthening community hardiness and personal resilience to provide the optimum opportunity for recovery from the crisis.
- Determine which populations will be unable to receive general public health emergency messages through mass communication channels during the initial phase of a public health emergency.
- Analyze the ways that information technology and new media influence communication decisions and pandemic preparedness.

Los Angeles Studies Paris Attacks

In April, Los Angeles sent a multi-agency delegation to Paris to meet with their French counterparts in law enforcement, intelligence, and public safety to learn about the November 2015 attacks. They identified best practices and lessons learned, bringing those findings home to apply to plans and training, publishing them in a White Paper.

"The Attacks on Paris - Lessons Learned: a Presentation of Findings" looks at six areas: intelligence, community engagement, investigation, incident command, crisis communication, and training/equipment. The paper provides a summary of the attacks in Paris, discusses prior attacks in France, and other high-profile attacks in Europe.

Any community looking to bolster its planning, response, and recovery efforts for such an attack should consider reading this concise 32-page White Paper. The lessons learned talk about differences in the way the two countries manage these incidents, point out weaknesses in the current systems that can easily be addressed, and what authorities learned and changed from prior attacks.

http://www.hsdl.org/?abstract&did=794337

Cybersecurity Guide for Law Enforcement Agencies

The National Consortium for Advanced Policing released "Cybersecurity Guide for State and Local Law Enforcement" (PDF, 1.3 Mb), a much-needed addition to the body of information available to law enforcement on cybercrimes. The guide is intended to help state and local law enforcement agencies protect themselves from cyber-crimes while also responding to cyber threats reported in the community.

https://cchs.gwu.edu/sites/cchs.gwu.edu/files/downloads/NCAPCybersecurityGuide-2016.pdf

Cybersecurity takes on more significance for law enforcement due to the nature of the work. In addition to malware and viruses, unsecure information within networks can lead to case information being stolen or even altered. The guide discusses successful attacks against law enforcement agencies and the types of threats they face.

Also available is an issue brief on the same topic, "A Policy Roadmap to Enhance Capabilities" (PDF, 736 Kb), which focuses on what policymakers can do to improve the cyber authority and capabilities of state and local law enforcement.

These documents makes this murky subject more accessible to law enforcement agencies, and prioritizes the steps agencies can take toward cybersecurity.

https://cchs.gwu.edu/sites/cchs.gwu.edu/files/downloads/NCAP%20CCHS%20Issue%20Brief%20FINAL_0.pdf

(Source: Law Enforcement Cyber Center http://www.iacpcybercenter.org/)

"Pokémon GO: The One Serious Problem Everyone Should Worry

About"

Popular Game a Problem for Authorities, Business By now, you've very likely seen or heard stories about the downsides of the popular new augmented-reality game Pokemon Go. There are reports of assaults, robberies, injuries, and even stabbings and sexual assaults in the short time since the game's release. One young woman even found a dead body.

These all increase emergency calls, but first responders have other things to watch for with this game. As players hunt for virtual Pokemon, they will be drawn into areas that their cellphone maps tell them to go, which may lead them into restricted areas on public or private property. This includes reports of trespassers at fire stations, military bases, critical infrastructure sites, and detention and rehabilitation centers. In addition to trespass calls, this can increase the potential for surveillance and suspicious activity reporting.

Employers are also trying to manage both employees playing on company time and the cyber threat that comes with increased presence and use of personal devices. The game requires so much access to your phone's features that, should a hacker gain access with malware, they would get ahold of a great deal of personal or business information. In addition, because so many people are using Google accounts to log in, hackers may be able to exploit a flaw allowing access to Google accounts without permission. Workplaces may want to review "Bring Your Own Device" policies.

If your public or private sector location is currently an unwilling piece of the Pokemon Go universe, you can attempt to "opt-out" using this form on the developer's website. Players can also opt-out of allowing the game to have so much access to their data.

(Source: Forbes: http://www.forbes.com/sites/bernardmarr/2016/07/19/pokemon-go-the-one-serious-problem-everyone-should-worry-about/#26567127297e)

FEMA Urges Americans to Be Prepared for Extreme Heat, Download FEMA Smartphone App *Residents to Download FEMA Smartphone App Designed to Help Families Before, During, and After Disasters*

 The Federal Emergency Management Agency (FEMA) is urging residents across the nation to take steps now to prepare their families and communities for extreme heat, by reviewing important safety information and downloading the FEMA smartphone app.

The National Weather Service announced today that "dangerously hot and humid conditions are expected this week across a large portion of the nation." Additionally, NOAA's Climate Prediction Center's latest outlook notes that most of the continental United States is facing elevated chances of well-above-average summer temperatures. According to the Centers for Disease Control & Prevention, heat kills more people than hurricanes, lightning, tornadoes, earthquakes and floods.

To help Americans stay safe during extreme heat, FEMA urges residents to consider taking the following actions in affected areas:

- Postpone outdoor games and activities and limit exposure to the sun.
- Drink plenty of water and avoid caffeine; limit alcoholic beverage intake.
- Dress in loose-fitting, lightweight and light-colored clothing.
- Spend the warmest part of the day in temperature-controlled buildings such as libraries, schools, movie theaters, shopping malls, or community facilities.
- Check on family, friends, and neighbors who do not have air conditioning and who spend much of their time alone.

FEMA also urges residents to download and use the free FEMA app, which provides valuable safety tips to help families prepare for and recover from more than 20 natural and man-made hazards. The FEMA app enables users to receive weather alerts from the National Weather Service for up to five locations across the nation, making it easy to follow severe weather that may be threatening family and friends. The app also provides family communication plans, customizable checklist of emergency supplies, and maps of open shelters and disaster recovery centers. The app is available on the Apple App Store and on Google Play.

To learn more about what to do before, during and after severe weather, visit www.Ready.gov.

Follow FEMA online at www.fema.gov/blog, www.twitter.com/fema, www.facebook.com/fema and www.youtube.com/fema. Also, follow Administrator Craig Fugate's activities at www.twitter.com/craigatfema. The social media links provided are for reference only. FEMA does not endorse any non-government websites, companies or applications.

FEMA's mission is to support our citizens and first responders to ensure that as a nation we work together to build, sustain, and improve our capability to prepare for, protect against, respond to, recover from, and mitigate all hazards.

NGOs: Filling gaps in Disaster Planning, Response and Recovery

Disaster response and recovery requires a coordinated effort between various public, private and nongovernmental organizations (NGOs) in order to be effective. And planning must involve everyone from these various sectors in order to ensure a coordinated response and recovery effort. Often, well-known NGOs are thought of and included, such as the Red Cross and the Salvation Army. **READ MORE**

Handling the threat of drones on your campus

As if security managers didn't have enough to worry about during major events on campus, drones are becoming an increasingly common problem. Hobbyists and other people using drones for recreational purposes see events as opportunities to take photos and capture action from unique angles. Although drones could also be used for more insidious purposes, the vast majority of drones that officers encounter are being operated by innocent, if reckless, civilians. **READ MORE**

1. Deadline is Aug. 5 to apply for participation in Aug. 23-25 FEMA's EMI Virtual Tabletop Exercise on 'Mass Casualty Incident'

The Federal Emergency Management Agency (FEMA)'s Emergency Management Incident Virtual Tabletop Exercise, set for Aug. 23-25, 2016, 12:00-4:00 p.m. will address mass casualty incident awareness and information sharing during response efforts to assist affected communities. Virtual Tabletop Exercises are offered at 10-15 participating locations. They are designed for a community-based group of 10 or more whole community representatives from your local emergency management community of practice. The exercises are hosted from EMI and connected to remote sites through the FEMA video teleconference bridge. Obtain details online, and be sure to apply by Aug. 5, 2016. Direct any questions to Doug Kahn or call 301-447-7645.

2. DHS Countering Violent Extremism Grant Webinars

The Department of Homeland Security (DHS) will host two webinars on the 2016 Countering Violent Extremism (CVE) grant program. The webinars will be offered from **2:00 to 3:00 p.m. EDT on both, Wednesday, July 20 and Monday, July 25.**

For the first time, non-governmental organizations (NGOs) will be eligible for DHS funding in order to promote community resilience against the threat of violent extremism.

The scheduled webinars will provide assistance to NGOs and higher education institutions in understanding the grant program's goals. Additionally, the webinars will present the opportunity to ask questions about the information presented.

Register for either webinar through the following links and complete the registration prior to the start of the sessions.
Sign up for July 25 webinar

In addition, participants may listen to the webinars by dialing **1-800-320-4330, pin 265976#.**

For more information on the CVE Grant Program, visit https://www.dhs.gov/cvegrants.

3. FEMA National Training Program Continuing Grants

FEMA announced funding opportunities for the Fiscal Year 2016 Continuing Training Grants program. The Homeland Security National Training Program's Continuing Training Grants will provide $11.5 million to qualified applicants to help improve the nation's ability to respond to and recover from all-hazard events.

The grants are administered by FEMA's National Training and Education Division and will be available for awards in four focus areas:
• Cybersecurity
• Hazardous Materials
• Economic Recovery
• Rural Preparedness

This highly competitive program attracts applicants from state, local, tribal, and territorial governments, eligible non-profit organizations, and higher education institutions. Funding is provided as cooperative agreements and awarded directly to the selected applicants.

For more information and to download the application package, visit www.grants.gov and submit applications no later than **August 22**.

4. EMI Offers Course Simulating Emergency Operation Centers

FEMA congratulates Fond du Lac County, Wisconsin, for completing their Integrated Emergency Management Course (IEMC). Fond du Lac's course was designed specifically for their jurisdiction, providing both lecture and exercised-based training focused on response operations for a train derailment resulting in a hazardous materials incident and an ecological disaster that affects a large recreational lake.

IEMC courses simulate realistic crisis situations that emergency operations center personnel and community leadership/elected officials may encounter during disasters or other events. Also, the course helps enhance the skills of participating officials, and provide a forum to evaluate the effectiveness of their specific emergency policies, plans, and procedures that protect life and property. The course's target audience includes state, local, tribal, and territorial government personnel; their elected and appointed officials; supervisory, operations,

and emergency support personnel; nonprofit organizations; the private sector; law enforcement personnel; firefighters; attorneys; public information officers; planners; and more.

IEMC classes are principally delivered at FEMA's Emergency Management Institute at the National Emergency Training Center in Emmitsburg, Maryland; however delivery may occur in the community. Questions should be directed to FEMA-EMI-IEMB@fema.dhs.gov. If your jurisdiction is interested in applying for the program and obtaining information on the application process and its timeline, please visit http://training.fema.gov/iemc/.

5. EMI Virtual Tabletop Exercise for Mass Casualty Incident

FEMA's Emergency Management Institute (EMI) is offering a virtual tabletop exercise (VTTX) focusing on Mass Casualty Incident (MCI) on **August 23-25 from 12:00 pm to 4:00 pm EDT.** This VTTX addresses MCI awareness and information sharing during response efforts to assist affected communities.

This VTTX allows participating communities to share details and best practices regarding mass casualty awareness, integration into all-hazard preparedness, information sharing, incident management, and resource management processes. The goals of the VTTX are to enhance the participants' knowledge, skills, and abilities to effectively conduct all-hazards emergency response and recovery. The VTTX also enables coordination of response operations with counterparts from federal agencies, state and local governments, private sector organizations, non-governmental agencies, and other whole community partners.

EMI conducts a monthly series of a VTTX using a Video Teleconference (VTC) platform to reach community-based training audiences around the country providing a virtual forum for disaster training. The VTTX is designed for a group of ten or more representatives from state, local, tribal, and territorial emergency communities of practice. Participants will need to connect through a site that is equipped with appropriate VTC capability, but alternate ways to participate are also available upon request. Session content is the same each day and participants only need to attend one session.

Interested individuals should email Doug Kahn at douglas.kahn@fema.dhs.gov or call 301-447-7645. Additionally, it is requested that individuals send a courtesy copy email to the Integrated Emergency Management Branch at FEMA-EMI-IEMB@fema.dhs.gov or call 301-447-1381. The deadline for VTTX applications is **August 5** and additional information can be found by visiting https://training.fema.gov/programs/emivttx.aspx.

6. FEMA Posts Draft Individuals and Households Program Unified Guidance for Public Comment

On June 15, 2016, FEMA posted the draft Individuals and Households Program Unified Guidance (IHPUG) to the Federal Register for public comment. FEMA strongly encourages the

public and emergency management community to submit comments. The Individuals and Households Program (IHP) is the most publicly recognizable FEMA program and this is an excellent opportunity for the public to provide their input.The draft guidance is posted to the Federal Register, and will be available for comment until **August 1, 2016**.

7. Apply for the 2017 National Emergency Management Executive Academy

The objective of the Executive Academy is to engage, challenge and enhance the talents of emergency management executives through critical thinking, visionary strategic planning, and negotiation and conflict resolution when applied to complex real-world problems. The Executive Academy consists of four resident sessions, webinars, distance learning, and literature reviews. Executives will explore how they can leverage science, technology, engineering, and data analysis to impact critical decisions and guide informed policy development. Executives will have the opportunity to work collaboratively on projects, share smart practices, and participate in exercises on cascading and catastrophic events.

Applications will be accepted through **August 5, 2016**. There are a limited number of seats and enrollment is competitive. For more information on the Executive Academy and the application and selection process, visit www.training.fema.gov/EMPP/executive.asp.

The Executive Academy is the pinnacle of a three-level Academy series in the Emergency Management Professional Program (EMPP) which includes Basic, Advanced, and Executive Academies. Emergency management professionals should visit the EMPP page for more information about which academy best suits their needs.

8. Draft Disaster Resilience Indicators Concept Released By Mitigation Federal Leadership Group Subcommittee

FEMA, National Oceanic and Atmospheric Administration (NOAA) and their federal partners in the Mitigation Federal Leadership Group (MitFLG) Disaster Resilience Indicators Subcommittee released a "Draft Interagency Concept for Community Resilience Indicators and National-Level Progress Measures."

This concept is the result of a year-long effort to identify potential indicators of community resilience capacity building that align with the Mitigation and Recovery Core Capabilities under the National Preparedness Goal. Learn more details about this joint FEMA/NOAA initiative here www.fema.gov/community-resilience-indicators.

The document, compiled in response to broad public interest in identifying key factors of community resilience nationwide in order to promote better-informed capacity building strategies, is intended to start a broad conversation among public- and private-sector stakeholders on how best to define and track improvements in community resilience capacity across 28 key indicator categories.

Interested stakeholders seeking to add their input can submit comments and feedback to the Disaster Resilience Indicators Subcommittee of the MitFLG at FEMA-CommunityResilience@fema.dhs.gov by **August 15, 2016**.

The MitFLG subcommittee was led by representatives of FEMA and the National Oceanic and Atmospheric Administration and includes significant contributions from federal partners such as the National Institute of Standards and Technology, the U.S. Army Corps of Engineers, and the U.S. Geological Survey.

Russell Fox
Branch Chief, Analysis and Integration
FEMA Region II/DHS
World Trade Center 1 (WTC1), 52nd Floor
New York, NY 10278
917-318-4859 Cell

http://www.fema.gov/continuity-operations
http://www.fema.gov/es/continuidad-de-operaciones